EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL

Ensuring High Assurance of EUDI Wallets
& the NL National eID Scheme

NL-CS-part2

NL EUDI Wallet Certification System

NL FITCEM Cybersecurity Certification Scheme
Scheme Procedures
NP002

RC1.0

2026.10.25

Document reference	NL-CS (part2)
Version	RC1.0
Status	Release Candidate
Date	25/10/2026
Document type	FITCEM Certification Scheme Scheme Procedures
Parent framework	NL-SYS-01, NL-SYS-02, NL-SYS-03, NL-SYS-04, NL-SYS-05 NL-TL
Scheme Owner	Kingdom of the Netherlands Minister of Economic Affairs
Certification target	European Digital Identity Wallet Solutions
Primary audience	Scheme Owners, Evaluation Laboratories; CABs, EUDI Wallet providers
Secondary audience	EUDI Wallet ecosystem stakeholders
Assurance level <identity proofing CIR 2015/1502> and <evaluation, EU Regulation 2019/881>	High/High
Related & Subsidiary Documents	NL-CS (part1, part3, part4) NL-CS-WI & NL-CS-WI-conditions NL-WSCA & NL-WSCA-conditions

NP002 sets out the operational procedures for certification under the NL FITCEM scheme for the European Digital Identity Wallet: application, evaluation planning, evaluation, certification decision, surveillance, change management, incident handling, suspension and withdrawal, recertification and scheme maintenance. It implements the policy of [NP001]. Where this document and [NP001] differ, [NP001] prevails and the difference is to be corrected here.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Version	Date	Summary of change
RC1.0	24 October 2026	Cleanup for publication

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Contents

Document control 2
1. Introduction 6
1.1 Purpose and relationship to NP001 6
1.2 Scope 6
1.3 Terms and scheme type 6
1.4 References 6
2. Application for certification 9
2.1 Eligibility 9
2.2 Selection of a Certification Body 9
2.3 Application submission 9
2.4 Application review 10
3. Evaluation planning 11
3.1 Evaluation plan 11
3.2 Evaluation Laboratory selection and licensing floor 11
3.3 Architecture verification 11
3.4 Sampling rules 12
4. FITCEM evaluation process 13
4.1 Overview 13
4.2 Evaluation evidence 13
4.3 Evaluation tasks 13
4.5 Product identity verification and delta assessment 14
4.6 Evaluation review meetings 15
4.7 Evaluation Technical Report 15
5. Review of dependencies 16
5.1 Purpose 16
5.2 Scope 16
5.3 Acceptability criteria 16
6. Certification decision 17
6.1 Certification assessment 17
6.2 Grounds for a positive decision 17
6.3 Certificate of conformity 17
6.4 Certification report and publication 17
6.5 Notification of the supervisory body 18
6.6 Complaints and appeals 18
7. Post-certification 19
7.1 Certification lifecycle 19
7.2 Surveillance evaluations 19
7.3 Special evaluations 20
7.4 Change management 20
8. Incident and vulnerability management 21
8.1 Notification by the product developer 21

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

8.2 Vulnerability management policy 21
8.3 Vulnerability impact analysis 21
8.4 Disclosure 21
8.5 Response by the Certification Body 21
9. Non-conformity, suspension and withdrawal 22
9.1 Consequences of non-conformity 22
9.2 Suspension 22
9.3 Withdrawal 22
9.4 Non-compliance by a Certification Body 22
10. Recertification 23
11. Scheme maintenance 24
12. Open points of this document 25
Annex A: Certification process summary 26
Annex B: Glossary 27
Annex C: FOR REVIEW and placeholder register 28

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

1. Introduction

1.1 Purpose and relationship to NP001

This document (NP002) contains the procedures that Certification Bodies (CB), Evaluation Laboratories and product developers follow when applying for, performing and maintaining certification of the European Digital Identity Wallet under the NL FITCEM scheme. [NP001] is the complete scheme document: it holds scheme policy, roles, the security requirements approach, the evaluation methodology and the certification process. NP002 does not restate that policy. It adds the procedural detail, and it refers to [NP001] by section number.

Instructions with a narrower audience are issued separately: [NI002] instructs Evaluation Laboratories on the evaluation tasks, and [NI003] instructs Certification Bodies on the audit of the product developer's operational processes.

1.2 Scope

- Application for certification and the acceptance review.
- Evaluation planning, including laboratory selection, architecture verification and sampling.
- The FITCEM evaluation process, including product identity verification and delta assessment.
- Review of the dependencies on components outside the Target of Evaluation.
- The certification decision, the certificate, the certification report and publication.
- Post-certification: surveillance, special evaluations, change management, incident and vulnerability management.
- Non-conformity, suspension and withdrawal; complaints and appeals; recertification; scheme maintenance.

1.3 Terms and scheme type

Terms follow [NP001], Annex A. Compared with the earlier draft: the ITSEF is the Evaluation Laboratory; the Wallet Provider that applies for certification is the product developer (eligibility is in section 2.1); the "NCCA [to be confirmed]" is replaced by the Scheme Owner, whose identity is still to be confirmed, because the Scheme Owner cannot be the supervisory authority [stated as position of R. Huisman in the project record; see [NP001] section 3.1].

1.4 References

External documents are referred to in the text by their reference tag. Versions, editions and dates are given only in this table. Legal acts cited by name, such as Regulation (EU) No 910/2014, Regulation (EU) 2024/1183 and Regulation (EC) No 765/2008, are not versioned.

Reference	Document	Version or date
[NP001]	NP001-EUDIW-C, NL FITCEM EUDI Wallet Certification Scheme (complete scheme)	0.9.4 for review, 24 October 2026
[NP002]	NP002, Scheme Procedures	0.9.4 for review, 24 October 2026

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Reference	Document	Version or date
[NI002]	NI002, Evaluation Instruction for Evaluation Laboratories	0.9.4 for review, 24 October 2026
[NI003]	NI003, Audit Instruction for Operational Processes	0.9.4 for review, 24 October 2026
[PP-WI-REMOTE]	FITCEM Protection Profile for EUDI Wallet Instance supported by a remote WSCA-WSCD (FITCEM-PP-WALLET-INSTANCE-for-REMOTE-WSCA-WSCD)	0.2d, 20 August 2026, draft
[PP-WI-DRAFT]	EN 17640 Protection Profile of the Wallet Instance (project draft; cryptographic annex pending)	Draft 0.6 reviewed; 0.7 pending
[TP-WI-BB]	Black-Box Penetration Testing Plan for the Wallet Instance, with effort estimate. Effort basis, not an evaluation test specification	1.0, 16 October 2026
[EN 17640]	EN 17640, Fixed-time cybersecurity evaluation methodology for ICT products (FITCEM)	2022
[EN 17927]	EN 17927, Security Evaluation Standard for IoT Platforms (SESIP)	2023
[ISO/IEC 15408]	ISO/IEC 15408, Evaluation criteria for IT security (Common Criteria)	2022
[ISO/IEC 18045]	ISO/IEC 18045, Methodology for IT security evaluation	2022
[ISO/IEC 17025]	EN ISO/IEC 17025, Competence of testing and calibration laboratories	2017
[ISO/IEC 17065]	EN ISO/IEC 17065, Requirements for bodies certifying products, processes and services	2012
[ISO/IEC 17067]	EN ISO/IEC 17067, Fundamentals of product certification	2013
[ISO/IEC 30111]	EN ISO/IEC 30111, Vulnerability handling processes	2019
[ISO 19011]	EN ISO 19011, Guidelines for auditing management systems (informative)	Edition not pinned
[EUCC-NI002]	Dutch NCCA EUCC scheme document NI002, Content and presentation of evaluation review meetings (reference only, Common Criteria terms)	1.0
[EUCC-NI003]	Dutch NCCA EUCC scheme document NI003, EUCC licensing evidence (reference only)	Dated 04-10-2024
[NSI002]	NSI002, Content and presentation of evaluation review meetings, EUDI Wallet certification using FITCEM (outside the NP001 document set)	1.0
[IR 2981]	Commission Implementing Regulation (EU) 2024/2981, certification of European Digital Identity Wallets (national certification schemes)	OJ L, 4.12.2024
[IR 2979]	Commission Implementing Regulation (EU) 2024/2979, integrity and core functionalities of European Digital Identity Wallets	2024

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Reference	Document	Version or date
[IR 848]	Commission Implementing Regulation (EU) 2025/848, registration of wallet-relying parties	2025
[OWASP MAS]	OWASP MASVS, MASWE, MASTG, MAS testing profiles (L1, L2, R, P) and the EUDI Wallet profile	MASVS 2.1.0; MASWE 1.0; MASTG current; EUDI Wallet profile draft, not released
[ARF]	EUDI Wallet Architecture and Reference Framework, including the Functional Conformance Assessment Framework	Version to be pinned

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

2. Application for certification

2.1 Eligibility

Only providers referred to in Article 5a(2) of Regulation (EU) No 910/2014 as amended by Regulation (EU) 2024/1183 are eligible to be issued a certificate under this scheme ([IR 2981], requirement for national certification schemes on eligibility). The CB verifies eligibility as part of the application review.

2.2 Selection of a Certification Body

The product developer selects a CB from the register of authorised Certification Bodies maintained by the Scheme Owner ([NP001] section 3.1). There is no restriction on cross-border engagement of authorised Certification Bodies. [Carried from the earlier draft; not addressed in [NP001].]

2.3 Application submission

The product developer submits the application to the selected CB. The application contains at least the following.

#	Element	Requirements
1	FIT ST (Wallet Security Specification)	Claims conformance to the applicable Protection Profile ([PP-WI-REMOTE] for the remote WSCA-WSCD variant) and instantiates it for the product ([NP001] section 4.1). Mirrors, without restating, the environmental requirements table of the Protection Profile ([NP001] section 2.4). Identifies the functional certificate as in row 3.
2	Architecture description	Identifies the architecture variant of [NP001] section 2.3, every component inside the TOE and every component assumed in the operational environment, including the WSCA-BE and the WSCD. A variant for which no Protection Profile is admitted cannot be applied for (section 3.3).
3	Functional certificate	A valid functional certificate, or attestation under the ARF Functional Conformance Assessment Framework, and where available the functional conformity assessment report, for the same product and the exact same version as submitted ([NP001] sections 3.4 and 6.2). The FIT ST identifies it by issuing body, certificate identifier, date of issue, validity period, and product and version covered.
4	Proposed evaluation plan	Scope, build and version identifiers, intended Evaluation Laboratory, timeline, target devices and variants proposed for sampling (section 3.4).
5	Risk assessment	The product developer's risk assessment that complements the scheme risk assessment and identifies risks and threats specific to the implementation, with treatment measures for all relevant risks. It is shared with the CB for evaluation ([IR 2981], requirements on national certification schemes, risk assessment by the provider).
6	Assurance information for components outside the TOE	Certificate and assurance report of the WSCD, and of the WSCA-BE where it is not part of the TOE, as listed in the environmental requirements of the Protection Profile (section 5).

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

#	Element	Requirements
7	Source code access	Source code is made available to the Evaluation Laboratory as required by the Protection Profile ([NP001] section 3.4). Failure to provide it counts as an evaluation failure [stated decision of the scheme owner].
8	Evidence per the checklist	The evidence listed in the evidence checklist of [NI002] section 3, or a statement of when each item will be delivered.
9	Operational process descriptions	Version control, change management, update delivery and vulnerability management, including the vulnerability management policy per [ISO/IEC 30111]. Input to the audit of [NI003].
10	Baseline information (changed products only)	Where the product differs from a previously certified product or from the product covered by the functional certificate, the baseline and change description needed for a delta assessment ([NP001] section 6.6, Annex C items 1 to 7).

2.4 Application review

The CB reviews the application within a reasonable time and confirms in writing, or states what is missing, that:

- the product developer is eligible (section 2.1);
- the FIT ST is sufficiently complete to proceed and claims conformance to an admitted Protection Profile;
- the architecture variant is admitted under [NP001] section 2.3;
- the functional certificate identifies the product, version and build as stated in the FIT ST, and is valid at the date of review ([NP001] section 6.2);
- the proposed evaluation plan is consistent with the scheme and the laboratory scope meets section 3.2;
- the assurance information for the components outside the TOE is present and plausible, subject to the full review of section 5.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

3. Evaluation planning

3.1 Evaluation plan

After acceptance the CB prepares the evaluation plan with the product developer and the Evaluation Laboratory and approves it in writing before the evaluation starts. The plan contains at least:

- the scope: product and version, build and release identifiers, architecture variant, platform versions and target devices, and the sampling approach (section 3.4);
- the FITCEM evaluation tasks of section 4.3 and the fixed time budget per evaluation task, set per [NP001] section 5.3 (the effort table of [NP001] is still a placeholder; the hours basis of [TP-WI-BB] is one input);
- the Evaluation Laboratory and confirmation that its accredited scope meets section 3.2;
- the pinned versions of the Protection Profile and of every referenced external specification, including each OWASP MAS deliverable and its draft status ([NP001] sections 4.4 and 6.1, phase 2);
- the test to requirement mapping, or the date on which it will be delivered ([NP001] section 4.3);
- the language of the Setup and User Guide (SUG) and the other evidence;
- the treatment of a finding that terminates the evaluation, and the custody of test tools between attempts (section 4.4);
- the timeline: delivery of evidence, evaluation tasks, the optional evaluation review meetings (section 4.6), the process audit ([NI003]), and the ETR.

3.2 Evaluation Laboratory selection and licensing floor

The CB engages one or more Evaluation Laboratories that act under its responsibility. The CB verifies, before approving the evaluation plan, that each laboratory:

- holds [ISO/IEC 17025] accreditation from a National Accreditation Body pursuant to Regulation (EC) No 765/2008, with an accredited scope covering the evaluation activities for the European Digital Identity Wallet at assurance level high ([NP001] section 3.3);
- meets the laboratory licensing floor of [NP001] section 3.3: an accredited scope covering either Common Criteria evaluation ([ISO/IEC 15408] with [ISO/IEC 18045]) at EAL4 with AVA_VAN.3 or higher, or SESIP evaluation ([EN 17927]) at SESIP level 3 or higher, and including the evaluation of mobile applications;
- is not relying on accreditation under EN ISO/IEC 17020, 17021 or 17029 as a substitute.

The CB keeps the accreditation certificate and the accredited scope statement on file and informs the Scheme Owner of the engagement for the register.

3.3 Architecture verification

The CB verifies that the architecture of the product submitted for evaluation matches the architecture described in the application, and that the evaluation plan proposed with the implementation matches the plan on which the application was based ([IR 2981], Article 13(2)). The CB also verifies that the architecture variant is admitted under [NP001] section 2.3. Today only the remote WSCA-WSCD variant is admitted. For the embedded secure element and eSIM variants a Protection Profile is required before certification, and the no dedicated secure element variant is not admitted at assurance level high. Where a product

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

developer proposes an architecture for which no Protection Profile is admitted, the CB informs the Scheme Owner and does not accept the application.

3.4 Sampling rules

Where the product exists in several variants, for instance per operating system version, device category or regional build, the CB defines sampling rules that avoid repetition of identical evaluation activities and focus on what is specific to a variant. Functional and security tests may be performed on a sample of variants and on a sample of target devices; the CB justifies the use of sampling in the evaluation plan ([IR 2981], Article 13(3)). The rules ensure that:

- tests are performed on a representative sample of variants and target devices;
- variant-specific activities concentrate on the elements that differ;
- the plan states which variants are covered by which sample evaluation.

A variant that changes the TOE boundary, the assumptions on the operational environment or the architecture variant is not a sampling case; it is treated under [NP001] section 6.6.

4. FITCEM evaluation process

4.1 Overview

The evaluation is performed by the Evaluation Laboratory under the responsibility of the CB, within the fixed time budget of the evaluation plan, under FITCEM ([EN 17640]) and [NP001] section 5. The assurance level is high and this is mandatory. The attack potential expectation and the depth of the vulnerability analysis (working position AVA_VAN.3) remain a placeholder in [NP001] section 5.1 and are not set here. The detailed instruction to the laboratory is in [NI002].

4.2 Evaluation evidence

The product developer provides all evidence of the evidence checklist ([NI002] section 3) to the Evaluation Laboratory in accordance with the evaluation plan. Completeness is verified in the first evaluation task. The evidence includes at least the FIT ST, the development documentation of the checklist, the SUG, test samples or test instances of the Wallet Instance with the accounts or backend access needed to operate them, the source code, the vulnerability and patch management process documentation, the risk assessment, the functional certificate, and the assurance information of section 5. Updates of evidence made necessary by findings are subject to the change rules of section 7.4.

4.3 Evaluation tasks

The evaluation tasks required at assurance level high are those of [EN 17640], Table 1 and Table D.2, as applied by [NP001]. The task numbers below are the clause numbers of [EN 17640] [checked against the standard text held in the project].

Task	EN 17640 evaluation task	Applicable at high	Key requirements in this scheme
6.1	Completeness check	Required	All evidence of the [NI002] checklist is present. Missing or incomplete items are findings and are reported to the CB. The product identity verification of section 4.5 starts here.
6.4	FIT Security Target evaluation	Required	Work units 1a and 1b: the FIT ST is well constructed and consistent and, because a Protection Profile is mandatory, all operations of the Protection Profile have assigned values. Confirms conformance to the Protection Profile, that the environmental requirements are mirrored, that the TOE boundary is unambiguous, and that the functional certificate is identified as required by [NP001] section 6.2.
6.5	Development documentation	Required	Complete analysis of the entries of the scheme-specific checklist: functionality, development process including vulnerability and patch management, design at module level, security architecture, source code. Kept light as [EN 17640] advises, with the source code available.
6.6	Evaluation of TOE installation	Required	Installation and set-up as described in the SUG, including backend test accounts, and a statement in the ETR on whether the TOE is in its secure state afterwards.

Task	EN 17640 evaluation task	Applicable at high	Key requirements in this scheme
6.7	Conformance testing	Required, full coverage	Complete conformance testing against the security claims of the FIT ST with the scheme-defined acceptance criteria, keyed to the Protection Profile requirements. No reduction on the basis of functional conformity testing ([NP001] section 6.2).
6.10	Penetration testing	Required	Flaw Hypothesis Methodology. The required test set is built on OWASP MAS ([NP001] section 4.4). Performed within the fixed time budget. Attack potential per [EN 17640] Annex F, expectation per [NP001] section 5.1 (placeholder).
6.12	Extended cryptographic analysis	Required	Cryptographic specification and its implementation. The cryptographic catalogue and methodology of this scheme are not yet defined; see the placeholder below.
-	Product identity verification	Required by [NP001] section 6.2.1	Performed by the laboratory and recorded in the ETR (section 4.5).
-	Delta assessment	Where [NP001] section 6.6 applies	Performed by the laboratory, reviewed by the CB (section 4.5).
-	Reporting	Required	ETR per Annex G of [EN 17640] (section 4.7).

The following tasks of [EN 17640] are not required at assurance level high: 6.3 review of security functionalities, 6.8 vulnerability review, 6.9 vulnerability testing and 6.11 basic cryptographic analysis (superseded by 6.12) [inferred from Table 1 and Table D.2, which list the tasks for high without them]. Evaluation of a FIT Protection Profile is a dedicated process and not part of the evaluation of a TOE ([EN 17640], note 1 to Table 1); the Protection Profile of this scheme is evaluated before it is admitted.

[PLACEHOLDER] cryptographic analysis. Extended cryptographic analysis ([EN 17640] task 6.12) needs a cryptographic catalogue or methodology reference. The project record states that the cryptographic annex is deferred to a later draft of the Wallet Instance Protection Profile [PP-WI-DRAFT]. Until it is issued, task 6.12 is required but its method is undefined.

4.5 Product identity verification and delta assessment

The Evaluation Laboratory verifies and records in the ETR that the submitted product is the same product, at the same version, as the product covered by the functional certificate, using the steps of [NP001] section 6.2.1 and [NI002] section 4.1. The CB does not take a positive certification decision without a positive identity result or, where the identifiers differ, a positive delta conclusion that the CB has reviewed and accepted.

Where the identifiers differ, or where the product differs from a previously certified product, the laboratory produces a delta assessment with the evidence of [NP001] Annex C and one of the conclusions covered, partially covered or not covered. The CB reviews it and may reject the conclusion and require it to be treated as not covered. The delta assessment is performed within the fixed time budget of the affected tasks; if it cannot be completed within that budget the conclusion is not covered. A delta assessment is not used where the change alters the TOE boundary, the assumptions on the operational environment, the environmental requirements, or the identity or version of a certified component on which the

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

product depends, and the changes listed in [NP001] section 6.6 are not concluded as covered without new analysis and testing of the affected requirements.

4.6 Evaluation review meetings

An evaluation review meeting (ERM) is optional ([NP001] section 6.1, phase 5). The CB decides in the evaluation plan whether and when ERMs are held. The CB chairs an ERM, which brings together the CB, the Evaluation Laboratory and, where the CB so decides, the product developer, in person or virtually. Its purposes are to confirm that the evaluator understands the TOE, to challenge the test plan and the test to requirement mapping before testing, and to confirm completeness of the evaluation and the draft ETR. The deliverables, the progressive checklist of evaluator actions and the roles of the evaluator and the certifier are in [NI002] section 5. The CB documents the outcome of each ERM.

4.7 Evaluation Technical Report

On completion of all tasks the Evaluation Laboratory submits the ETR to the CB. The ETR follows Annex G of [EN 17640] and also records:

- the time spent per evaluation task and any deviation from the evaluation plan;
- a verdict per task and every finding with its assessed severity;
- the result of the product identity verification, and the delta assessment where there is one;
- the test to requirement mapping with the target requirement of every test and the module it exercises;
- the identity, version and validity of the WSCD certificate and of any other certified component recorded as an environmental requirement ([NP001] section 5.4);
- the tool and platform versions used, and the OWASP MAS versions used;
- whether the TOE meets the security claims of the FIT ST and whether the FIT ST is conformant to the Protection Profile.

The CB reviews the ETR for completeness and accuracy and may request clarification or supplementary information from the laboratory before the certification decision.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

5. Review of dependencies

5.1 Purpose

The review determines whether the assurance information for components that are not evaluated as part of the TOE is available and adequate for the intended use in the wallet solution ([IR 2981], recital on dependency analysis). Its basis is the product developer's risk assessment and the assumptions of the FIT ST on the operational environment.

5.2 Scope

Under the draft Protection Profile the Wallet Instance is a standalone TOE; the WSCA-BE and the WSCD are in the operational environment and key protection and cryptographic operations are required to be performed inside a certified WSCD/WSCA ([NP001] sections 2.1 and 2.4). The certificate of the WSCD is therefore an environmental requirement and not a composition input. The CB reviews at least:

- the WSCD certificate: that it is valid, that its identity and version are as stated in the FIT ST, that the assessment is at assurance level high as required by Annex IV, section 2 of [IR 2981], and that its scope, operating environment assumptions and user guidance are compatible with the intended use;
- the WSCA and WSCA-BE assurance information against Annex IV, section 3 of [IR 2981], in particular that the recommendations in the user guidance are compatible with the conditions of use in the wallet solution and that the assumptions made about WSCAs are covered by the assurance information;
- the mechanisms by which the Wallet Instance verifies, for each wallet unit, that the end user device satisfies the assumptions on the platform (Annex IV, section 4 of [IR 2981]). These mechanisms are security controls and are evaluated at the assurance level of the Wallet Instance;
- any other certificate or assurance documentation relied upon, assessed against the criteria of Annex II of [IR 2981].

The Evaluation Laboratory records the identity, version and validity of each such certificate in the ETR ([NP001] section 5.4). Where the product developer has a justification for an exception to the vulnerability assessment of the WSCD or WSCA, the product developer notifies the Scheme Owner ([IR 2981], recital on exceptions to the vulnerability assessment; Annex IV).

5.3 Acceptability criteria

For each piece of assurance documentation the CB assesses the type and validity period, the competence and impartiality of the issuing body, whether its scope is adequate for the intended use within the wallet solution, and whether the assurance level is sufficient relative to the scheme. Where the information for the WSCD or WSCA is incomplete or inconclusive, the CB requires the product developer to specify compensating requirements or deems the component unsuitable for this certification.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

6. Certification decision

6.1 Certification assessment

The certifying function of the CB assesses the ETR, any delta assessment, the dependency review and the audit report of [NI003]. The assessment is performed independently of the evaluation activities.

6.2 Grounds for a positive decision

A positive decision may be taken where:

- all evaluation tasks of section 4.3 are completed with positive verdicts;
- all findings are resolved, or accepted with documented justification, and any termination under section 4.4 has been followed by a completed re-run;
- the product identity result is positive, or a delta conclusion is positive and has been reviewed and accepted by the CB (section 4.5);
- a functional certificate for the same product and the exact same version is valid at the date of the decision ([NP001] section 6.2);
- the dependency review of section 5 is positive;
- the initial audit of the operational processes under [NI003] is positive;
- the FIT ST reflects the evaluated product accurately and completely;
- no open vulnerability precludes certification at assurance level high.

6.3 Certificate of conformity

The CB issues the certificate of conformity with the content specified in Annex VII of [IR 2981] [referred to by Article 14(1)(a)], and in addition:

- the product developer and the certified product, with version and build identifiers;
- the scope, including the architecture variant, the Protection Profile identification and version, and any sampling limitation;
- the functional certificate by issuing body, certificate identifier, date of issue, validity period, and product and version covered ([NP001] section 6.2);
- the assurance level, the date of issue and the expiry date;
- the CB and the Evaluation Laboratory with their accreditation references;
- the Trust Mark [to be confirmed] as the only mark of conformity.

The validity does not exceed five years, as laid down in Article 5c(4) of Regulation (EU) No 910/2014.

6.4 Certification report and publication

With the certificate the CB prepares and publishes the public certification report, including at least a summary of the evaluation activities, scope and findings, as set out in Annex VIII of [IR 2981] [referred to by Article 14(1)(b)]. The report records the functional certificate identifiers of section 6.3. The certification assessment report, with the more detailed evaluation results, is provided to the Scheme Owner and may be made available to the Cooperation Group and to the Commission (Article 14(2)). The CB notifies the Scheme Owner of the issued certificate for the public register ([NP001] section 6.3).

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

6.5 Notification of the supervisory body

Certification Bodies notify the supervisory body referred to in Article 46a(1) of Regulation (EU) No 910/2014 of the issuance, suspension and cancellation of certificates of conformity ([IR 2981], Article 11).

6.6 Complaints and appeals

The CB handles complaints and appeals relating to its implementation of the scheme or to a certificate it issued in the first instance ([NP001] section 3.2). The procedure informs the complainant of progress and of the decision, and of the right to an effective judicial remedy. Complaints and appeals that have not been, or cannot be, resolved by the CB are sent to the Scheme Owner for assessment and resolution ([IR 2981], Article 15). [Escalation to the Scheme Owner is not yet stated in [NP001] section 3.2.]

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

7. Post-certification

7.1 Certification lifecycle

The lifecycle follows the reference schedule of Annex IX of [IR 2981] [checked against the project text]. It is a recommendation; other schedules are possible as long as the validity does not exceed five years, and each evaluation is performed within 12 months of the evaluation of the previous year.

Year	Evaluation	Mandatory activities
0	Initial	Full evaluation of the Wallet Instance including vulnerability assessment and the update feature of each software component. Evaluation of the maintenance processes, excluding their operating effectiveness ([NI003], initial audit). Certificate of conformity issued; start of the 4-year cycle.
1	Surveillance	Operating effectiveness of the maintenance processes: at least version check, update and vulnerability management ([NI003]). Evaluation of changes impacting the security of the product.
2	Surveillance	Vulnerability assessment of the full solution. Operating effectiveness of the maintenance processes. Evaluation of changes impacting the security of the product.
3	Surveillance	Operating effectiveness of the maintenance processes. Evaluation of changes impacting the security of the product.
4	Recertification	Full evaluation including vulnerability assessment; simplified evaluation for features and processes that have not changed. Update feature of each software component. Evaluation of the maintenance processes including operating effectiveness. New certificate of conformity.

In addition, the vulnerability assessment is performed at least every two years in surveillance evaluations and covers at least the changes in the product and in the threat environment since the last one. Penetration testing is added in case of an increased risk level or the emergence of new threats (Annex IX, point 1).

7.2 Surveillance evaluations

The CB conducts or oversees the surveillance evaluations according to the schedule above and [NI003]. They address the operating effectiveness of version control, update delivery and vulnerability management, the review of all changes since the last evaluation using the delta assessment of section 7.4, the updated vulnerability assessment where scheduled or triggered, and the continued validity of the functional certificate and of the certificates listed as environmental requirements. The CB issues a surveillance report to the product developer. If continued conformity is confirmed the certificate remains valid; if not, section 9 applies. The CB monitors the product developer's compliance with its obligations under the scheme and the conformity of the certified product ([IR 2981], requirement on monitoring by the CB).

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

7.3 Special evaluations

A special evaluation may be triggered at the demand of the CB or of the certificate holder following a significant change to the product or to the threat environment (Annex IX, point 4). In this scheme the triggers are:

- a change concluded as partially covered or not covered under section 7.4;
- an identified vulnerability or incident affecting the product;
- suspension, withdrawal or expiry of the functional certificate, or a change of identity, version or certification status of the WSCD ([NP001] sections 6.5 and 6.6);
- a request of the product developer before expiry of the certificate;
- a decision of the CB or the Scheme Owner on the basis of a change in the threat environment.

A special evaluation may lead to a new certificate of conformity with the same expiry date as the original (Annex IX, point 5). The CB determines its scope in consultation with the product developer.

7.4 Change management

The product developer notifies the CB of all planned changes to the certified product before implementation ([NP001] section 3.4). Wallet instances change often: variants follow the platform, and updates are frequent ([IR 2981], Annex IV, section 5). The CB determines for each change whether it is covered by a special evaluation or by the verification of the operating effectiveness of the maintenance processes ([IR 2981], Article 18(3)). This scheme uses the delta assessment of [NP001] section 6.6 and Annex C for that purpose, replacing the minor, significant and major classes of the earlier draft.

Delta conclusion	Required action
Covered	Recorded by the CB. The change is examined in the next surveillance evaluation as part of the operating effectiveness of the maintenance processes.
Partially covered	Special evaluation of the affected requirements and modules within the fixed time budget of the affected evaluation tasks. Results for the remainder are reused.
Not covered	Full evaluation. Where the certificate is to be retained, a special evaluation with the same expiry date; otherwise a new certification.

The changes that [NP001] section 6.6 says shall not be concluded as covered without new analysis and testing apply in full. The CB records its decision and informs the product developer in writing.

8. Incident and vulnerability management

8.1 Notification by the product developer

The product developer notifies the CB without undue delay of any breach or compromise of the certified product that is likely to impact its conformity ([IR 2981], Article 5(2)). Under [NP001] sections 3.4 and 6.4, critical vulnerabilities and active exploits are notified within 24 hours of discovery and high-severity vulnerabilities within 72 hours, and other vulnerabilities and changes follow the timeline of the scheme. The notification contains a description, the affected components, the potential impact on security properties and the initial remediation steps. The criteria on the impact of vulnerabilities and changes that determine notification (Article 5(4)) are the severity classes of this section; the severity scale is [to be defined, FOR REVIEW].

8.2 Vulnerability management policy

The product developer establishes, maintains and operates a vulnerability management policy and procedures taking into account [ISO/IEC 30111] (Article 5(3)). Article 5(7) of the same Regulation requires the policy to meet the requirements of Annex I to the Cyber Resilience Act.

8.3 Vulnerability impact analysis

For any vulnerability that affects the software components of the wallet solution the product developer prepares a vulnerability impact analysis report (VIAR) covering the impact on the certified product, the risks associated with the proximity or likelihood of an attack, whether the vulnerability can be remedied using available means, and possible ways to remedy it (Article 5(5)). The VIAR is transmitted to the CB without undue delay (Article 5(6)).

8.4 Disclosure

The product developer discloses and registers any publicly known and remediated vulnerability in the online repositories referred to in Annex V of [IR 2981] (Article 5(9)). Article 5(8) requires national schemes to establish vulnerability disclosure requirements applicable to Certification Bodies.

8.5 Response by the Certification Body

On receipt of a notification or a VIAR the CB assesses the impact on the conformity of the certified product, determines whether a special evaluation is required, reports the incident or vulnerability to the Scheme Owner regardless of severity ([NP001] section 3.2), and notifies the supervisory body of any suspension (section 6.5). The CB suspends the certificate without undue delay after it confirms that the notified breach or compromise impacts conformity (Article 12(1)). The Scheme Owner maintains the central vulnerability register and issues guidance ([NP001] section 6.4).

9. Non-conformity, suspension and withdrawal

9.1 Consequences of non-conformity

Where the CB establishes non-conformity of the certified product, by surveillance, special evaluation, notification or otherwise, it (Article 17):

1. informs the product developer and requests remedial actions within a defined timeframe;
2. informs other relevant market surveillance authorities where the non-conformity concerns other Union legislation;
3. sets the conditions for carrying out the remedial actions and monitors them;
4. restores the certificate, if suspended, when conformity is confirmed restored;
5. withdraws the certificate where the non-conformity is irreparable or not remedied in time.

9.2 Suspension

The CB suspends a certificate where a vulnerability or incident affecting the security properties is confirmed and remediation is pending, where required notifications, surveillance cooperation or evidence are not provided, where a change that requires evaluation was implemented without it, where the functional certificate is suspended or withdrawn, or where continued conformity is otherwise in reasonable doubt. Suspension is communicated to the product developer, the Scheme Owner and the supervisory body without undue delay and is shown in the public register. The CB states the conditions for restoration.

9.3 Withdrawal

The CB withdraws a certificate (cancellation in [IR 2981]) where the non-conformity cannot be remedied or is not remedied in time, in particular a suspended certificate after a breach that has not been remedied in a timely manner, or a vulnerability not remedied commensurately with its severity and potential impact (Article 12(2) and (3)). Withdrawal also follows where the product developer requests it, ceases to operate or discontinues the product. The Regulation notes that cancellation can have severe consequences, up to revocation of all deployed wallet units, and the CB only considers it where an unremedied vulnerability is likely to significantly affect the reliability of the wallet solution or of another wallet solution (recital 19). Withdrawal is communicated to the product developer, the Scheme Owner and the supervisory body, published in the register, and the product developer stops using the Trust Mark.

9.4 Non-compliance by a Certification Body

[PLACEHOLDER] consequences for a CB. Article 17 of [IR 2981] requires the scheme to set out the consequences of non-compliance by the Certification Body with the scheme requirements. The earlier draft and [NP001] are silent. Candidate content: powers of the Scheme Owner to suspend or withdraw the authorisation of a CB, treatment of certificates already issued, and the link to the National Accreditation Body. To be decided.

10. Recertification

The product developer may request recertification before the certificate expires ([IR 2981], Article 18(2)). Recertification follows the full procedure of this document with the simplifications of Annex IX: a full evaluation including vulnerability assessment, with a simplified evaluation of features and processes that have not changed, an update feature for each software component, and an evaluation of the maintenance processes including operating effectiveness. Reuse of earlier results is justified by a delta assessment with the previous evaluation as baseline ([NP001] section 6.6), and all conditions of that section apply, including the re-assessment of the attack potential in the light of the elapsed time (Annex C items 16 and 17). A functional certificate for the exact version must be valid at the decision.

A new certificate is issued after a successful recertification with a validity of at most five years from its date of issue. The CB notifies the product developer at least 12 months before expiry [carried from the earlier draft; not in NP001].

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

11. Scheme maintenance

The Scheme Owner maintains the scheme as set out in [NP001] section 6.7 and Article 6 of [IR 2981]. This comprises: governance of the definition of the scheme and its requirements; timelines for issuing certificates after an updated version is adopted, both new and previously issued; a periodic review that takes into account requests for clarification addressed to the Scheme Owner, feedback from stakeholders and the responsiveness of the Scheme Owner to requests for information; monitoring of reference documents with transition periods; a process to ensure the latest risks and threats in the risk register of Annex I are covered; and a process for other changes. For each revision the transition arrangements of [NP001] section 6.7 are published, and the Cooperation Group is notified where required.

Reference documents monitored: [EN 17640]; [EN 17927]; [ISO/IEC 17065], [ISO/IEC 17025], [ISO/IEC 17067] and [ISO/IEC 30111]; Regulation (EU) 2024/1183; [IR 2979], [IR 2981] and [IR 848]; [ARF]; [PP-WI-REMOTE]; and each [OWASP MAS] deliverable named in [NP001] section 4.4.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

12. Open points of this document

The FOR REVIEW and placeholder boxes of this document are collected in Annex C. Points that originate in [NP001] are not resolved here; they are listed so that they are resolved there first.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Annex A: Certification process summary

The phases are those of [NP001] section 6.1.

#	Phase (NP001 6.1)	Step	Responsible	Section
1	Application	Eligibility, selection of CB	Product developer	2.1, 2.2
1	Application	Application submission including functional certificate	Product developer to CB	2.3
1	Application	Application review and written acceptance	CB	2.4
2	Evaluation planning	Evaluation plan, laboratory verification against the floor	CB with laboratory and developer	3.1, 3.2
2	Evaluation planning	Architecture verification, sampling rules	CB	3.3, 3.4
3	FITCEM evaluation	Delivery of evidence	Product developer to laboratory	4.2
3	FITCEM evaluation	Tasks 6.1, 6.4, 6.5, 6.6, 6.7, 6.10, 6.12; product identity; delta assessment	Laboratory under CB	4.3, 4.5
3	FITCEM evaluation	Findings and termination	Laboratory, CB	4.4
3	FITCEM evaluation	Review of dependencies	CB	5
4	Process audit	Initial audit of operational processes	CB	[NI003]
5	Evaluation Review Meeting	Optional ERMs	CB chairs	4.6
3	FITCEM evaluation	ETR	Laboratory to CB	4.7
6	Certification decision	Decision, certificate, certification report, notifications	CB certifying function	6.1 to 6.5
7	Post-certification	Surveillance years 1 to 3, special evaluations, change management	CB, product developer	7
7	Post-certification	Incident and vulnerability management; suspension and withdrawal	Product developer, CB	8, 9
7	Post-certification	Recertification (year 4)	CB, product developer, laboratory	10

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Annex B: Glossary

Terms of [NP001] Annex A apply. Additional terms:

Term	Definition
CAR	Certification assessment report. Detailed report of the evaluation results, provided to the Scheme Owner and available to the Cooperation Group and the Commission.
ERM	Evaluation review meeting. Optional meeting chaired by the CB to review the state of the evaluation. Section 4.6 and [NI002] section 5.
Evaluation Laboratory	Laboratory fulfilling [ISO/IEC 17025] that performs the evaluation tasks under the responsibility of the CB. Formerly ITSEF.
Product developer	The provider of the wallet solution that applies for and holds the certificate of conformity. Formerly Wallet Provider.
Scheme Owner	Party that owns and governs the scheme. Identity [to be confirmed]. Formerly "NCCA [to be confirmed]" in the earlier draft.
Supervisory body	The supervisory body referred to in Article 46a(1) of Regulation (EU) No 910/2014, notified by Certification Bodies under Article 11 of [IR 2981]. Not yet a role in [NP001] section 3.1.
VIAR	Vulnerability impact analysis report prepared by the product developer.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Annex C: FOR REVIEW and placeholder register

Section	Point	Origin
1.3	Scheme type: [NP001] says Type 5, [IR 2981] requires type 6	[NP001] sections 1.2, 6.1
1.4	[NSI002] outside the document set	NP002 / [NP001] section 7
2.4	Functional certificate before evaluation versus delta assessment in advance	[NP001] sections 3.4, 6.2, 6.6
3.2	CB umbrella route versus the floor (decision 8); no licensing procedure	[NP001] section 3.3
4.3	Cryptographic catalogue and method for task 6.12	[EN 17640] PP annex pending
4.4	Termination rule, restart budget, tool custody	[NP001] sections 5.2, 6.6
5.2	Platform assumptions versus the scope of platform testing	[NP001] section 2.2
6.5	Supervisory body missing from the parties	[NP001] section 3.1
7.4	Emergency security fixes versus approval before implementation; mapping of delta conclusions to actions	NP002
8.1	Severity scale for notification criteria	[NP001] sections 3.4, 6.4
8.2	CRA Annex I and the scope exclusion of [NP001]	[NP001] section 2.2
8.4	Vulnerability disclosure requirements for CBs	[IR 2981] Art. 5(8)
9.3	Suspension and withdrawal criteria and timeframes (EZU)	[NP001] section 6.5
9.4	Consequences of non-compliance by a CB	[IR 2981] Art. 17

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme